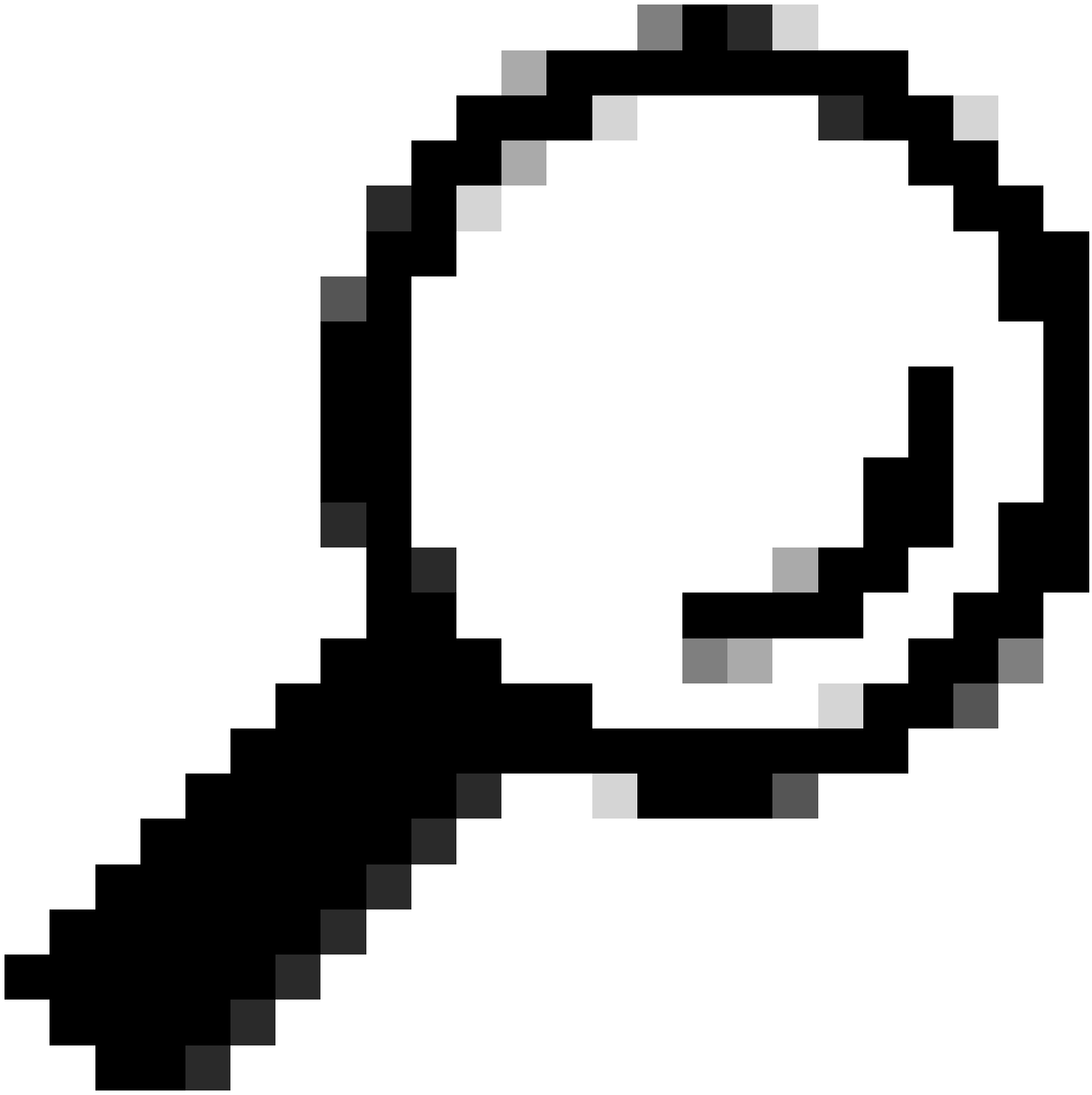
Secure Network Analytics Leitfaden zu externen Verbindungen

Inhalt

Einleitung

Verwenden Sie diesen Leitfaden, um externe Verbindungen zu überprüfen, die für den schnellen Betrieb bestimmter Funktionen von Secure Network Analytics erforderlich sind. Bei diesen externen Verbindungen kann es sich um Domänen oder Endpunkte handeln. Domänen sind Namen, die zur Identifizierung von Ressourcen im Internet, in der Regel Websites oder Dienste, verwendet werden; und Endpunkte sind tatsächliche Geräte oder Knoten, die über ein Netzwerk kommunizieren. Da der Schwerpunkt dieses Leitfadens auf Web-Services liegt, werden diese als URLs angezeigt. In der Tabelle sind die URLs der externen Verbindung in alphabetischer Reihenfolge aufgeführt.



Tipp: In der Tabelle sind die URLs der externen Verbindung in alphabetischer Reihenfolge aufgeführt.

Externe Verbindungen

URL der externen Verbindung	Zweck
https://analytics.int.obsrvbl.com	Wird von Secure Network Analytics für den Austausch von Telemetriedaten mit Secure Cloud Analytics-Services verwendet.
https://api.apj.sse.itd.cisco.com	Wird von Cisco für die

	Datenübertragung an Amazon Web Services (AWS) für den Asien-Pazifik-Raum, Japan und China (APJC) benötigt. Diese Funktion wird bei der Weiterleitung von Warnmeldungen an Cisco XDR sowie für Kennzahlen zum Kundenservice verwendet.
https://api.eu.sse.itd.cisco.com	Wird von Cisco für die Datenübertragung an Amazon Web Services (AWS) für die Region Europa (EU) benötigt. Diese Funktion wird bei der Weiterleitung von Warnmeldungen an Cisco XDR sowie für Kennzahlen zum Kundenservice verwendet.
https://api-sse.cisco.com	Wird von Cisco für die Datenübertragung an Amazon Web Services (AWS) für die Region USA benötigt. Diese Funktion wird bei der Weiterleitung von Warnmeldungen an Cisco XDR sowie für Kundenservice-/Erfolgsmetriken verwendet.
https://apix.cisco.com	Wird von Secure Network Analytics für die Funktion zum direkten Herunterladen von Software verwendet.
https://dex.sse.itd.cisco.com	Erforderlich für das Senden und Erfassen von Kundenerfolgskennzahlen
https://est.sco.cisco.com	Erforderlich für das Senden und Erfassen von Kundenerfolgskennzahlen

https://eventing-ingest.sse.itd.cisco.com	Erforderlich für das Senden und Erfassen von Kundenerfolgskennzahlen
https://feodotracker.abuse.ch/downloads/ipblocklist.txt	Wird von Threat Feed benötigt, der für Warnungen und Beobachtungen von Secure Network Analytics verwendet wird, wenn Analytics aktiviert ist.
https://id.cisco.com	Wird von Secure Network Analytics für die Funktion zum direkten Herunterladen von Software verwendet.
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/ip-filter.gz	Wird von Threat Feed benötigt, der für Warnungen und Beobachtungen von Secure Network Analytics verwendet wird, wenn Analytics aktiviert ist.
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/url-filter.gz	Wird von Threat Feed benötigt, der für Warnungen und Beobachtungen von Secure Network Analytics verwendet wird, wenn Analytics aktiviert ist.
https://lancope.flexnetoperations.com/control/lncp/LancopeDownload	Erforderlich für den Secure Network Analytics Threat Intelligence Feed, der für Warnungen und Sicherheitsereignisse von Secure Network Analytics verwendet wird. Hierfür ist die Secure Network Analytics Threat Intelligence Feed-Lizenz erforderlich.
https://mx*.sse.itd.cisco.com	Erforderlich für das Senden und Erfassen von Kundenerfolgskennzahlen
https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json	Ermöglicht den Zugriff auf MITER-Informationen für Warnungen, wenn

	Analytics aktiviert ist.
https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json	Ermöglicht den Zugriff auf MITER-Informationen für Warnungen, wenn Analytics aktiviert ist.
https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json	Ermöglicht den Zugriff auf MITER-Informationen für Warnungen, wenn Analytics aktiviert ist.
https://s3.amazonaws.com/onconfig/global-blacklist	Erforderlicher Bedrohungs-Feed, der für Warnungen und Beobachtungen von Secure Network Analytics verwendet wird, wenn Analytics aktiviert ist.
https://sensor.anz-prod.obsrvbl.com	Wird von Cisco für die Datenübertragung an Amazon Web Services (AWS) für den Asien-Pazifik-Raum, Japan und China (APJC) benötigt. Diese Funktion wird bei der Weiterleitung von Warnmeldungen an Cisco XDR sowie für Kennzahlen zum Kundenservice verwendet.
https://sensor.eu-prod.obsrvbl.com	Wird von Cisco für die Datenübertragung an Amazon Web Services (AWS) für die Region Europa (EU) benötigt. Diese Funktion wird bei der Weiterleitung von Warnmeldungen an Cisco XDR sowie für Kennzahlen zum Kundenservice verwendet.
https://sensor.ext.obsrvbl.com	Wird von Cisco für die Datenübertragung an Amazon Web Services (AWS) für die Region USA benötigt. Diese

	Funktion wird bei der Weiterleitung von Warnmeldungen an Cisco XDR sowie für Kennzahlen zum Kundenservice verwendet.
smartreceiver.cisco.com	Wird für den Zugriff auf Cisco Smart Software Licensing verwendet. Weitere Informationen finden Sie im Smart Licensing-Handbuch. Falls gewünscht, ist auch eine alternative Offline-Lizenzierung verfügbar. Weitere Informationen finden Sie in den Versionshinweisen.
https://software.cisco.com	Wird von Secure Network Analytics für die Funktion zum direkten Herunterladen von Software verwendet.
https://www.cisco.com	Erforderlich für die Cisco Domäne, die für Smart Licensing, Cloud-Proxy und Firewall-Verbindungstests verwendet wird.

Zusätzliche Informationen

Um genauer zu untersuchen, wie und warum bestimmte Domänen- und Endgeräteverbindungen verwendet werden, lesen Sie die folgenden Themen:

- Cisco Secure Service Exchange (SSE)
- Direkte Software-Downloads (Beta)
- MITER ATT&CK®-Framework
- Bedrohungs-Feed

Cisco Secure Service Exchange (SSE)

SSE-Endpunkte werden für die Datenübertragung an Amazon Web Services (AWS), von Cisco für Kennzahlen zum Kundenservice und auch für die Weiterleitung von Warnmeldungen an Cisco XDR verwendet. Diese variieren
basierend auf Region und Hosts. Diese Endpunkte werden dynamisch mithilfe eines Service Discovery-Mechanismus erkannt, der vom SSE Connector bereitgestellt wird. Bei der Veröffentlichung von Erkennungen in Cisco XDR versucht Secure Network Analytics, einen Service mit der Bezeichnung "xdr-data-platform" und seinem API-Endpunkt "Events" zu erkennen.

Region und Hosts

Je nach Region in Produktionsumgebungen sind die Hosts wie folgt.

USA:

- https://api-sse.cisco.com
- https://sensor.ext.obsrvbl.com

EU :

- https://api.eu.sse.itd.cisco.com
- https://sensor.eu-prod.obsrvbl.com

APJC:

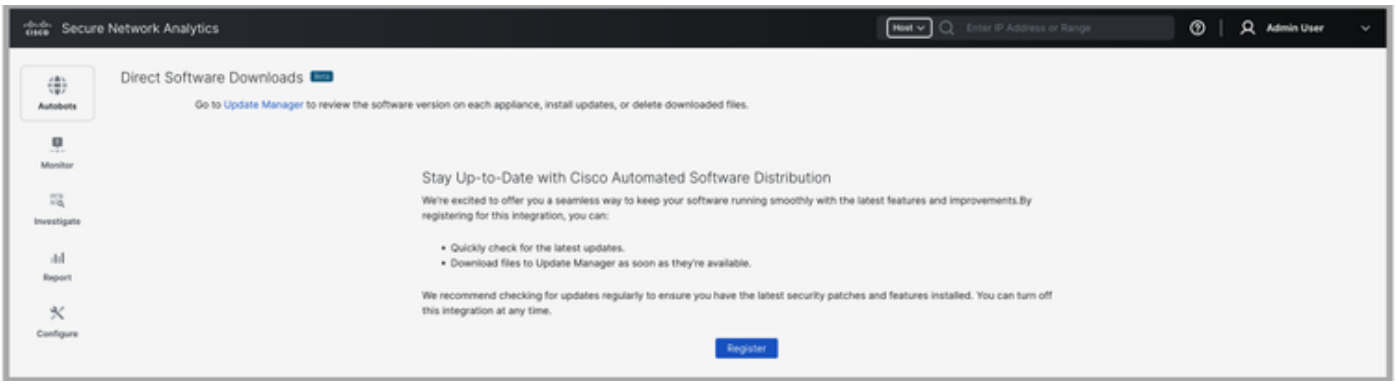
- https://api.apj.sse.itd.cisco.com
- https://sensor.anz-prod.obsrvbl.com

Direkte Software-Downloads (Beta)

Die folgenden Verbindungen werden von der Funktion für direkte Software-Downloads verwendet:

- https://apix.cisco.com
- https://software.cisco.com
- https://id.cisco.com

Um diese neue Funktion zum direkten Herunterladen von Software- und Patch-Update-Dateien in Ihren Update Manager zu verwenden, müssen Sie sich mit Ihrer cisco.com Benutzer-ID (CCOID) registrieren.
1. Melden Sie sich beim Manager an.
2. Wählen Sie im Hauptmenü Configure > Global > Central Management.
3. Klicken Sie auf die Registerkarte Update Manager.
4. Klicken Sie auf den Link Direct Software Downloads, um die Registrierungsseite zu öffnen.
5. Klicken Sie auf die Schaltfläche Registrieren, um den Registrierungsvorgang zu starten.

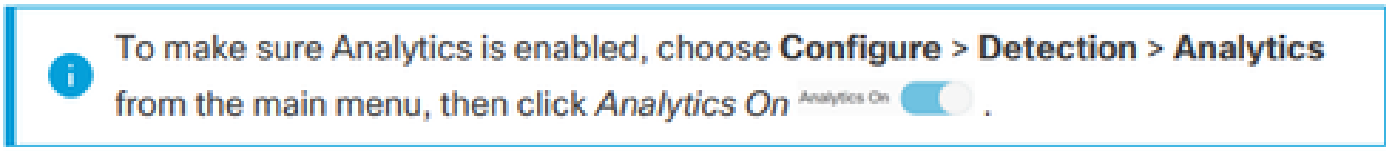


6. Klicken Sie auf den angegebenen Link.
7. Sie gelangen zur Seite "Activate Your Device" (Gerät aktivieren). Klicken Sie auf Weiter, um fortzufahren.
8. Melden Sie sich mit Ihrer cisco.com Benutzer-ID (CCOID) an.
9. Sie erhalten die Nachricht "Gerät aktiviert", sobald Ihre Aktivierung abgeschlossen ist.
10. Kehren Sie zur Seite "Direkte Software-Downloads" Ihres Managers zurück, und klicken Sie auf Weiter.
11. Klicken Sie auf die Links für die EULA- und die K9-Vereinbarung, um die Bedingungen zu lesen und zu akzeptieren. Wenn Sie die Bedingungen akzeptiert haben, klicken Sie auf Weiter.

Weitere Informationen zu direkten Software-Downloads erhalten Sie vom Cisco Support.

MITER ATT&CK®-Framework

Das MITER ATT&CK® Framework ist eine öffentlich zugängliche Wissensdatenbank von Taktiken und Techniken der Gegner, die auf realen Beobachtungen basieren. Wenn Sie in Secure Network Analytics die Option Analytics aktiviert haben, unterstützen die MITER-Taktiken und -Techniken die Erkennung und Reaktion von Cybersicherheitsbedrohungen.



Über die folgenden Verbindungen kann Secure Network Analytics auf MITER-Informationen zugreifen
für Warnungen:

- https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
- https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobileattack.json
- https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterpriseattack.json

Bedrohungs-Feed

Der Cisco Secure Network Analytics Threat Feed (ehemals StealthWatch Threat Intelligence Feed) stellt Daten aus dem globalen Threat Feed zu Bedrohungen für Ihr Netzwerk bereit. Der Feed wird regelmäßig aktualisiert und enthält IP-Adressen, Portnummern, Protokolle, Hostnamen

und URLs, die für schädliche Aktivitäten verwendet werden. Die folgenden Hostgruppen sind im Feed enthalten: Command-and-Control-Server, Bogons und Tors.

Um den Bedrohungs-Feed in der zentralen Verwaltung zu aktivieren, folgen Sie den Anweisungen in der Hilfe.

1. Melden Sie sich bei Ihrem primären Manager an.
2. Wählen Sie Configure > Global > Central Management.
3. Klicken Sie auf das Symbol (Hilfe). Wählen Sie Hilfe aus.
4. Wählen Sie Appliance-Konfiguration > Bedrohungs-Feed.

Weitere Informationen zu Threat Feed finden Sie im Systemkonfigurationshandbuch.

Support kontaktieren

Wenn Sie technischen Support benötigen, führen Sie einen der folgenden Schritte aus:

- Wenden Sie sich an Ihren Cisco Partner vor Ort.
- Support von Cisco
- So öffnen Sie ein Ticket über das Internet: http://www.cisco.com/c/en/us/support/index.html
- Für telefonischen Support: 1-800-553-2447 (USA)
- Für weltweite Support-Nummern: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.